Roundtable Discussion Topics

Samuel P. Jenkins

Director, Defense Privacy and Civil Liberties Office

April 28, 2010

Privacy Act Implementation Challenges

- Technology changes
- The Internet
- Easily portable mass storage (thumb drives, laptops, CDs)
- Faster and faster computer processing speeds
- Increased interconnectivity of computer systems
- Practically everyone has a computer
- Areas of Act difficult to interpret and apply in today's environment
- Definitions - What is personal information…personally identifiable information … PA protected information? How do we wrap our arms around it?
- Is there any system that does not retrieve by a personal identifier? Are we just engaging in wordplay?
- Is there pervasive abuse of ‘routine uses’?

Privacy Act Implementation Challenges

- The Act gives the Director of the Office of Management and Budget the power to develop regulations and guidelines on how agencies should implement the Act.
- The Act is 35 years old. Can it still effectively regulate the collection, maintenance, use, and dissemination of personal information by today's federal executive branch agencies?
  - Technology has progressed exponentially since 1975
  - Some areas of the Act are difficult to interpret and implement
  - What's so 'routine' about routine uses? What are 'compatible' purposes?

Privacy Act Implementation Challenges

The U.S. Privacy Protection Study Commission (1977)

- Did not result in the benefits Congress intended.
- Contained language that was unclear.
- Relied too heavily on the definition of a ‘system of record’ that was restricted to databases where information is retrieved by personal identifier.
- Required the publication of notices in the Federal Register that were ineffective since public readership is very limited and the notices lack sufficient detail.

Privacy Act Implementation Challenges

- **The 2008 GAO Report** Made Three Primary Findings
  - The GAO found that the definition of a “system of records” is not universally applicable to the types of personally identifiable information collected by the government. The GAO recommended revising this definition to cover all personally identifiably information that is collected by the federal government.
  - The GAO found that the current privacy regime does not adequately control collection and use of personally identifiable information. In response, the GAO recommended that the law be amended to require agencies to justify collection of information and to justify the use or sharing of personally identifiably information.
  - The GAO found that current methods used to inform the public about policies and practices around government collections of information are ineffective. Specifically, Privacy Act notices are hard to understand and difficult to find. The GAO recommended the use of layered notices, in which the most important facts are presented to the user to begin with, followed by denser and more esoteric information as the user digs deeper. The GAO also recommended publishing these sorts of notices at a central, easy to access location on the Web.

Privacy Act Implementation Challenges

The Information Security and Privacy Advisory Board found that:

The Privacy Act and related policy should be brought up to date.

- **Amendments to the Privacy Act of 1974 and Section 208 of the E-Government Act of 2002 are needed to:**
  - o Improve Government privacy notices;
  - o Update the definition of System of Records to cover relational and distributed systems based on government use, not holding, of records.
  - o Clearly cover commercial data sources under both the Privacy Act and the E-Government Act.

- **Government leadership on privacy must be improved.**
  - o OMB should hire a full-time Chief Privacy Officer with resources.
  - o Privacy Act Guidance from OMB must be regularly updated.
  - o Chief Privacy Officers should be hired at all "CFO agencies."
  - o A Chief Privacy Officers' Council should be developed.

- **Other changes in privacy policy are necessary.**
  - o OMB should update the federal government's cookie policy.
  - o OMB should issue privacy guidance on agency use of location information.
  - o OMB should work with US CERT to create interagency information on data loss across the government
  - o There should be public reporting on use of Social Security Numbers

Privacy Act Implementation Challenges

- **Installation Physical Access Control Systems (1 of 2)**
  - Is PII being collected? If yes, under what SORN?
  - Where is PII being stored? Are your contractors storing the data?
  - Is the ‘yes/no’ decision for entry being kept in a database?

Privacy Act Implementation Challenges

- **Installation Physical Access Control Systems (2 of 2)**
  - How is the individual advised if a decision to deny entry is determined?
  - What sources of information are being used in the access decision? Is it a government authorized source that is reliable, timely and accurate?

Privacy Act Implementation Challenges

- **Information Sharing Environment (ISE) (1 of 2)**
  - Composed of Five Communities
    - Intelligence
    - Law Enforcement
    - Defense
    - Homeland Security
    - Foreign Affairs

Privacy Act Implementation Challenges

- **Information Sharing Environment (ISE) (2 of 2)**
  - **Mission**
    - **to share terrorism-related information through trusted partnerships so those who have information can share it and those who need information receive it,**
    - **in order to improve information sharing among federal entities; state, local, and tribal entities; the private sector; and our foreign partners.**
  - **The Privacy framework establishes core privacy protections and enables information sharing while ensuring appropriate safeguards for privacy and civil liberties protection for Americans citizens.**
  - **More information to follow**

Privacy Act Implementation Challenges

- **Controlled Unclassified Information (CUI) (1 of 6)**
  - May 9, 2008 Presidential Memorandum mandates implementation of CUI framework within Information Sharing Environment (http://georgewbush-whitehouse.archives.gov/news/releases/2008/05/20080509-6.html)
  - "All departments and agencies shall apply the CUI Framework, … for the designation, marking, safeguarding, and dissemination of any CUI terrorism-related information within the ISE that originates in departments and agencies, regardless of the medium used for its display, storage, or transmittal."

Privacy Act Implementation Challenges

- **Controlled Unclassified Information (CUI) (2 of 6)**
  - NARA has been designated as the Executive Agent to implement the CUI framework (http://www.archives.gov/cui/about/cuio.html)
  - Three CUI designations replace “Sensitive But Unclassified (SBU)”

Privacy Act Implementation Challenges

- **CUI Designations (3 of 6)**
  - "Controlled with Standard Dissemination" meaning the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.

Privacy Act Implementation Challenges

- **CUI Designations (4 of 6)**
  - "Controlled with Specified Dissemination" meaning the information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.

Privacy Act Implementation Challenges

- **CUI Designations (5 of 6)**
  - "Controlled Enhanced with Specified Dissemination" meaning the information requires safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

Privacy Act Implementation Challenges

- **Controlled Unclassified Information (CUI) (6 of 6)**
  - The DoD has expanded the implementation of CUI to include all DoD CUI not just information that falls within the ISE.
    - OSD memorandum, “White House Approval of CUI Policy Framework”, July 21, 2008
    - USD(I) memorandum, “Clarification of Current DoD Policy on CUI”, April 7, 2009

SSNs

Reduction of the Use of Social Security Numbers required by OMB Memo M-07-16

- Eliminate Unnecessary Use. Agencies must now also review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months.22

- Explore Alternatives. Agencies must participate in government-wide efforts to explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs (*e.g.*, surveys, data calls, etc.).

Disclosure of the Social Security Number

- It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

- Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Privacy Act Implementation Challenges

- Social Security Number Use Reduction (1 of 2)
  - DoD Directive-Type Memorandum 07-015-USD(P&R) “DoD Social Security Number Reduction Plan”
  - At every juncture, question why we’re collecting the SSN
  - Review use of SSNs and justifications

Privacy Act Implementation Challenges

- Social Security Number Use Reduction (2 of 2)
  - Review existing and new forms
  - Submit annual report with FISMA report
  - Crosscheck system inventories and systems of records notices

Privacy Act Implementation Challenges

- **Web 2.0**

"*Web 2.0 is fundamentally social, treating the individual at the center of the universe as opposed to groups or organizations, and then basing communication and information paths on social relationships between individuals.*"

  - Stowe Boyd, DoD Web 2.0 Guidance Forum

Privacy Act Implementation Challenges

- **Web 2.0 Concerns**
  - Favorite target of hackers
  - Posting inappropriate content
    - Offensive language
    - PII (posting own or someone else's)
    - National security
  - Personnel must ensure information posted to official social networking site is approved for public use
  - Continuous monitoring is imperative

Privacy Act Implementation Challenges

- **Identity Theft**
  - Constant threat to our organization
  - Enforce awareness among personnel
  - Report all breaches to DPO
  - Conduct risk analysis to determine next steps in individual notification
  - FTC Identity Theft Site http://www.ftc.gov/bcp/edu/microsites/idtheft/

Privacy Act Implementation Challenges

- **Contractor Oversight (1 of 2)**
  - When an agency provides by contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of Section (m) to apply to such system, and
  - Any such contractor and any employee of such contractor shall be considered to be employees of an agency.

Privacy Act Implementation Challenges

- **Contractor Oversight (2 of 2)**
  - FAR 52.224-1 Privacy Act Notification http://www.defenselink.mil/privacy/files/sites_of_interest/FAR_52_224_1.pdf
  - FAR 52.224-2 Privacy Act http://www.defenselink.mil/privacy/files/sites_of_interest/FAR_52_224_2.pdf
  - DFAR Part 224 - Protection of Privacy and Freedom of Information http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars224.htm

OMB's Statutory Responsibilities Privacy Act of 1974

- **The Privacy Act states that "The director of the Office of Management and Budget shall…provide continuing assistance to and oversight of the implementation of this section by agencies."**
- **Guidance, Memos, consultation with agencies regarding Privacy Act inquiries**
- **Requires agencies to provide OMB with advance notice of new or significant changes to systems of records and matching programs.**
- **1975 Guidelines and Responsibilities/Circular A-130**
- **Comment on proposed legislation amending or affecting implementation of the Privacy Act.**

OMB's Statutory Responsibilities Privacy Act of 1974

- **The Privacy Act states that "With respect to privacy and security, the Director (of OMB) shall…develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies…"**
- **It also requires OMB approval for collections of information from the public and provides opportunity for the public to comment on proposed information collections.**

OMB's Statutory Responsibilities E-Gov Act of 2002

- **The Privacy Act states that "With respect to privacy and security, the Director (of OMB) shall…develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies…"**
- **It also requires OMB approval for collections of information from the public and provides opportunity for the public to comment on proposed information collections.**

Resources

- Privacy Act of 1974
- Federal Register July 9, 1975 Privacy Act Implementation-Guidelines and Responsibilities
- DOJ Overview of the Privacy Act of 1974, 2004 edition
- OMB Circular A-130
- Various OMB Memoranda
- Section 208 – E-Gov Act
- Federal Acquisition Regulations